Process Control
Security Requirements Forum
(PCSRF)

Security Capabilities Profile
for
Industrial Control Systems

September 17th, 2003

Industrial Control System Security Capabilities Profile
September 17th, 2003

1. Introduction

1.1. Initiative Purpose

The National Information Assurance Partnership (NIAP – partnership between the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST)), as part of the Critical Infrastructure Protection Program, provides technical support and guidance to industry to improve the information technology security posture of the systems and supporting operations that comprise the US national critical information infrastructure. One component of this effort addresses computer and communications security[1] for the networked digital process control systems used to provide or support industrial operations. The NIST Intelligent Systems Division of the Manufacturing Engineering Laboratory, the NIST Information Technology Laboratory and the NIST Electrical and Electronics Engineering Laboratory comprise this component, and are working with industry to incorporate the appropriate electronic security into process control systems and the components that comprise such systems.

The goal of this effort is to characterize the security capabilities to be provided by the product components that comprise an Industrial Control System (ICS), and the security capabilities that must be exhibited by the ICS after the product components have been integrated together to form an ICS. This effort is being carried out through the Process Control Security Requirements Forum (PCSRF). The outcome of this effort will be a set of security capabilities that can be applied by the control system industrial sectors to aid in the acquisition, integration, operation, and maintenance of ICSs.

The PCSRF is comprised of representative organizations from the various sectors that make up the US process control industry (i.e., vendors that design and develop components and systems, organizations that integrate components and systems for the industry, end-users of ICSs, and relevant standards organizations), as well as representatives from companies that use these systems. The PCSRF is working with control systems and security professionals to assess threats and potential vulnerabilities in order to establish appropriate strategies for the development of policies and countermeasures to be employed through combinations of technology and procedural mechanisms.

1.2. Document Purpose

The document addresses those issues associated with presenting and justifying a *security assurance case* as it applies to day-to-day ICS operations. The security assurance case

[1] Computer and Communication Security is inclusive of all devices implemented through combinations of hardware, software and firmware, and, which provide or support security-relevant functions of the industrial control system. These functions may also have indirect impact on safety-critical functions of the industrial control system.

serves exactly the same purpose as a safety assurance case[2]: it presents *claims* in regards to the critical capabilities that the system must possess; it provides a body of supporting *evidence* which illustrates that the critical capabilities have been achieved; it provides a set of arguments, or *rationale*, which links the claims to the evidence. The collection of claims, evidence and rationale enables demonstration of due diligence in justifying that an acceptable level of risk has been achieved.

The security assurance case focuses on presenting claims, evidence and rationale as follows:

- Statement of the Security Problem: Claims about the ICS are stated in the form of assumptions about the operational environment and intended use of the ICS, in the form of vulnerabilities in the ICS and the technologies and processes used to build, operate and maintain the ICS, and in the form of policies, directives and mandates to which the ICS must comply.

- Statement of the Solution to the Security Problem: Claims about the *protection mechanisms*[3] and *assurance measures*[4] deemed as necessary and sufficient to address the stated security problem are identified and described. The protection mechanisms can be stated in varying degrees of specificity; starting with a high-level statement of objectives, followed by intermediate-level statements of functional and assurance requirements, and finally low-level statements describing the implemented functions and assurance measures. These measures may be technological in nature or may be comprised of physical or procedural factors.

- Substantiation of the Solution: Rationale demonstrates complete traceability between the statements of the security problem down to the statements of the security solution. The rational also presents the argument that the implemented mechanisms as a whole are necessary and sufficient to solve the stated security problem.

A security assurance case generates a significant amount of information that must be organized for presentation to the various stakeholders involved with the development, verification and operation of the system once it becomes operational. The Common Criteria for Information Technology Security Evaluation (CC/ISO 15408) defines a security specification framework (called a Protection Profile) which provides a standardized template for organizing and specifying security criteria, and catalogs of

[2] Safety assurance cases are commonly used by mission-critical and safety-critical sectors (such as the military, industrial and aerospace sectors) to convey the reasoning and justification behind the engineered solutions upon which mission-critical or safety-critical operations depend.

[3] A protection mechanism may be implemented through a combination of technology-based (i.e. computer-based) mechanisms and procedural functions. With regard to computer-based mechanisms, they may in turn be implemented in any combination of hardware, software or firmware.

[4] Assurance measures are the activities conducted to reach a conclusion that the required capabilities have been implemented in accordance with their requirements. Assurance measures include the generation of evidence required to support the activities.

functional and assurance criteria that is used to populate the template. This document incorporates the concepts of an ISO 15408-compliant Protection Profile (PP) but differs from the PP in several ways:

1. This document contains information that exceeds the scope of information required in a CC-compliant Protection Profile;
2. This document has a structure that differs from a CC-compliant Protection Profile;
3. This document avoids the use of CC-specific terms and phrases.

NIST intends that this document will serve as a means to reach consensus within and across industries regarding the security capabilities present to secure an ICS. The document will serve as a vehicle to convey to the process control system and component vendors the security capabilities that are desired in new products for application in the ICS space. After that goal is met, this document and its derivatives will serve as a basis for developing ISO 15408-compliant Protection Profiles to aid in development and verification of the security capabilities of ICS systems and product components.

1.3. Scope of Application

This document discusses security issues and capabilities relevant to those industries regarded as components of the national critical information infrastructure. Candidate industries may include the electric utilities, discrete parts manufacturing, petroleum (oil & gas), water, waste, chemicals, pharmaceuticals, pulp & paper, and metals and mining.

1.4. Industrial Control System Definition

An ICS can be characterized as a distributed collection of components that provide the following basic functions to control a complex process:

- Measurement – data generation
- Acquisition – data collection
- Control – data assessment, information generation and response determination, and automatic or manual response
- Human-machine interface – processing of inputs from and presentation of information to human operators.

The functions described above are referred to as normal functions. While this document focuses on maintaining security for normal functions, it is also necessary to address the ability to install, configure and transition the ICS from a secure halted state to its secure normal state, to maintain security during abnormal states, and to transition from the secure normal or abnormal state to a secure shutdown/halted state. Some examples of these special functions/states associated with overall ICS operation include:

- startup, initial condition or set-point establishment

- System and process behavior management controls, discrete event logging, configuration and maintenance of the system and its components, and changes associated with new process equipment and ICS devices
- Failure modes, secure fail-over and secure recovery
- Shutdown
- Archive and backup

1.5. Understanding and Applying this Document

This section discusses the methods used to collect the information in this document and discusses application of this document to develop, integrate and operate secure ICSs.

1.5.1. How this Document was Developed

This document was developed through a series of technical information exchanges facilitated by NIST. The information exchanges were conducted through a variety of face-to-face meetings, teleconferences, workshops and industrial control system facility tours. Meetings, including teleconference meetings, have been convened at NIST headquarters, at industry conferences, at sector-specific workshops.

The purpose of these industry-focused information exchanges was to capture as much information as possible related to the present state of ICS operations. This type of information exchanges included:

- Discussion of fundamental principles of DCS, PLC and SCADA;
- Discussion of the unique aspects and characteristics of the technology employed in ICS as compared to the application of technology for more traditional computer and communications systems;
- Discussion of ICS vulnerabilities;
- Discussion of desired functionality and technology capability.

1.5.2. Intended Usage

This document defines a superset of security capabilities that would exist in electronic programmable components that comprise an industrial control system. Each operational ICS will need to apply these capabilities as appropriate for that system's environment. The security and safety risks of the operational environment of the ICS must be assessed for each ICS. Based upon the security and safety risks in which the ICS components must operate, individual security capabilities will be specified, configured, and employed by customers to meet the overall security needs of the ICS. The specific configuration of the components to support organizational security and safety objectives is left to the system designers to implement , For each selected capability, the specific requirements statements (shall statements) should be reviewed and modified to provide the desired level of functionality and assurance – in the same manner as requirements and assurance measures are selected to meet a Safety Integrity Level (SIL) as in IEC 61508.

Although the risks and vulnerabilities will vary with each ICS, the inherent security capabilities that can be optionally utilized to implement secure ICS applications can be assembled to facilitate:

- The establishment of acceptable ICS security criteria applicable across control system industries.

- The establishment of acceptable security criteria applicable to a single process control industry or single ICS installation.

It is envisioned that the applicability of this document and its derivatives to ICS industry security activities will grow over time. The information content and security capabilities described in this document should be used to support each of the following aspects of the ICS life-cycle:

- Acquisition of ICS Products – There are two ways in which this document may serve the acquisition process:

    1. Statement of required security capability – In this context, this document serves as the basis for communicating the required security functionality that must exist in candidate products. The vendor community would incorporate a subset of the security capabilities defined by the specification as appropriate for the specific device(s) they manufacture or integrate.

    2. Criteria to gauge sufficiency of available products – In this context the document serves as the basis for determining how well a candidate product meets the required security capabilities[5].

- Verification of Compliance – There are two ways in which this document serves as a basis for determining the conformance of an implementation[6]:

    1. Evaluation at the component level – The evaluation would serve to substantiate the conformance of the implementation of a well-defined set of security functions and mechanisms.

    2. Evaluation at the system level – The evaluation would serve to substantiate the conformance and suitability of the implementation for a well defined set of security functions within a well-defined operational environment and operational context.

[5] A byproduct of this activity is the ability to determine the "gap" that exists between what the product does and what is required. In the case where the product provides less capability, the information supports developing alternative measures. Where the product exceeds what is required, the opportunity exists to utilize that capability to further reduce risk.

[6] There remains the open question as to who would be the certification authority to oversee evaluations, and what organization(s) would be performing the evaluation.

In achieving any of the above goals it is important to recognize that a single security capabilities profile document can not be effective in addressing all the security issues and concerns of all US process control industries for each of the environments in which ICSs operate. At the industry sector level there may be further general agreement on recommended security policies and practices to guide implementation at the facility level. Within each control industry sector, this document must be refined, tailored and elaborated with increasingly detailed information that is specific to the state, region, or industrial control facility within which the ICS is being employed. In addition, only the ICS facility can fully provide details of the specific ICS components, architecture and day-to-day operational requirements to govern the secure operations and maintenance of that ICS.

This document and its derivatives will serve as the basis for developing ISO 15408 compliant Protection Profiles, these can then be tailored, elaborated with increasing detailed information for a specific instantiation of the recommended security capabilities which will then form a better basis for judging conformance of a specific implementation.

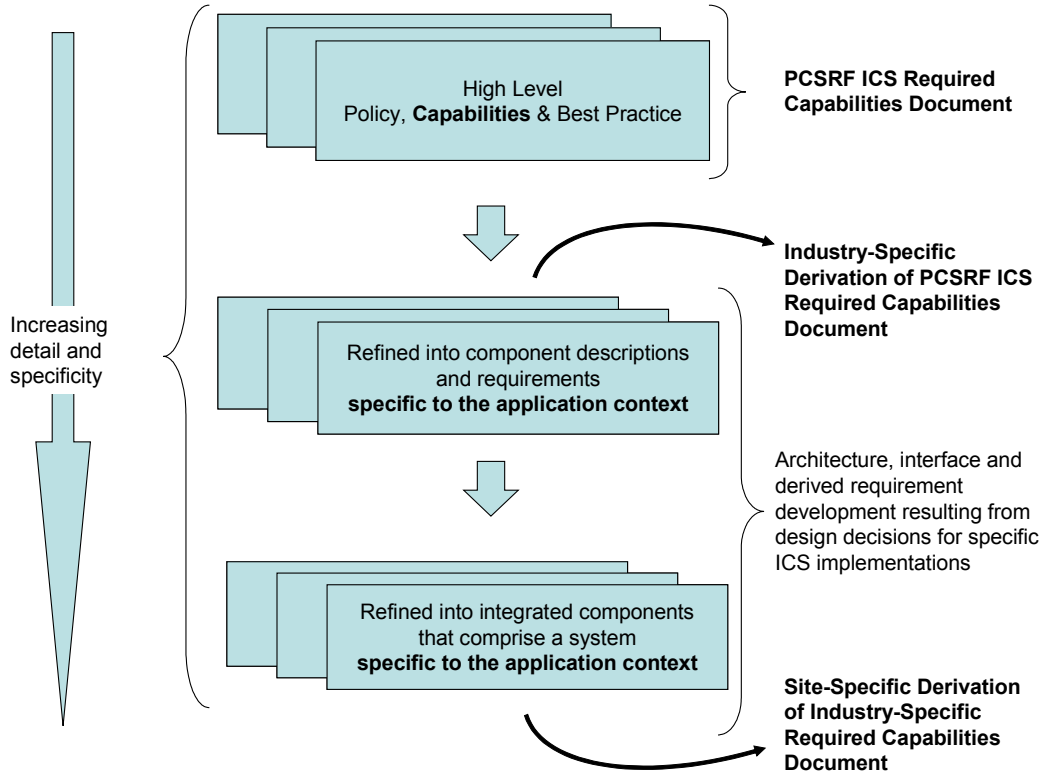


Figure 1 – Required Security Capabilities Document Refinement

This concept for application of the document is illustrated in Figure 1 and parallels that taken when developing an enterprise-wide security policy. Corporate management will establish high-level policies that are applicable across all organizations within the corporation. Each corporate site, division, or other operational entity will then refine the high level policy into operational procedures. This process repeats and terminates at the

lowest level of operation. It is only at the lowest level operation that the details specific to that operation can be stated with accuracy.

The scope of the PCSRF ICS SCP is to develop the superset of required security capabilities for Industrial Control Systems.

1.5.3. Difference between Capability and Configuration

The terms capabilities and configuration, as used in reference to the engineering of systems are often used interchangeably although they have very different meanings. Capabilities refer to the *potential* for performing an action whereas configuration refers to a *specific instance* or *manner* in which the potential is put into effect.

As an example, a firewall may have the capability, or potential, to allow or disallow information to flow inbound to an organization's protected network from an external unprotected network. The firewall may also have the capability, or potential, to allow only authorized individuals to create, delete and modify the rules that determine the types of information flow that are allowed and disallowed. A specific firewall product will be designed, implemented and tested to demonstrate that it provides the desired capabilities. However, once that firewall is installed in an operational network it must be configured to enforce the specific details of an organizations' network information flow policy. Such a policy may require that only those individuals operating in the network administrator role be allowed to create, modify and delete information flow enforcement rules. That same policy might also require that all inbound information flows are restricted unless they are a response to an outbound information flow. It is necessary to have two types of information: one to provides the statement of required capabilities and another to provides the statement of required operational configuration.

This document defines required capabilities but does not define any specific configuration of those capabilities in an operational context.

1.6. Relationship of this Document to other ICS Security Initiatives

Effective ICS security is implemented through application of comprehensive security-focused systems engineering, management, and operations and maintenance activities throughout the entire life-cycle of the ICS. This document focuses on security as it applies to a generic System Development Process as indicated in Figure 2. Figure 2 illustrated that this document is a receiver and provider of information and that there are concurrent security initiatives that provide information to or receive information from this document.

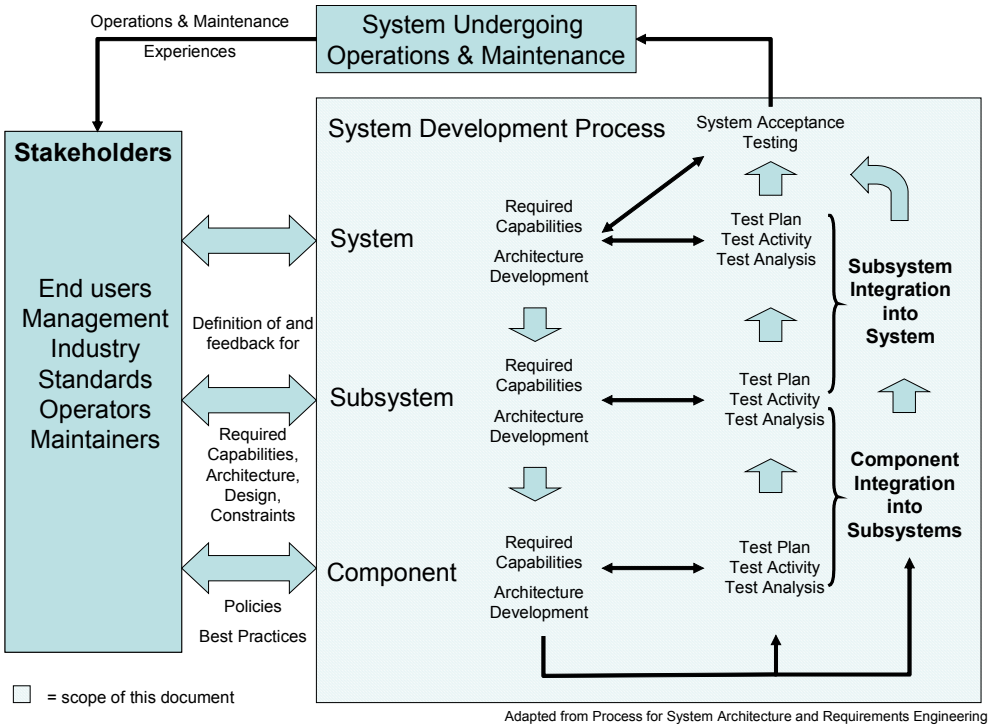


Figure 2 – System Life Cycle Activities

It is important to recognize that system development is an iterative process occurring simultaneously at several levels of abstraction: at the system level, at the subsystem level, and at the component or product level. This document defines ICS required capabilities independent of a specific architecture, at the ICS system level. The information in this document must be refined and tailored for each specific ICS in response to the details of the environment, the architecture, the subsystem definition and the components that comprise the subsystems**.**

1.6.1. Relationship with the PCSRF

The PCSRF provides the mechanism to facilitate information flow across control system sectors. This document and its protection profile derivatives are developed through the guidance and facilitation provided by the PCSRF.

1.6.2. Relationship with the Protection Profiles

The future Protection Profiles developed will be used to validate security compliance to the PCSRF security capabilities of the specific industry sector, instantiation of an ICS. The process control components and system can be acquired, tested and integrated into the ICS, and the ICS itself can be verified to be compliant with the security capabilities as stipulated in the Protection Profile, and thereby the PCSRF SCP.

1.6.3. Relationship with SP99

The SP99 committee is working to establish an information base consisting of background security information, application guidance, security technology surveys, and best security practices for instituting and maintaining a security program for ICSs, independent of specific industrial sectors. While the SP99 effort is broadly focused and comprehensive, it does not address all of the requirements associated with engineering security into a component or system at a level of detail sufficient to design or procure new equipment or services.

The relationship between SP99 and this document is best described as follows: SP99 provides general guidance on security based upon the risks and vulnerabilities. The PCSRF ICS SCP defines the required security capabilities of the ICS components or system that can be purchased for use in a *specific ICS operation.*

1.6.4. Relationship to NIAP & Common Criteria Recognition Arrangement (CCRA)

From this document, Common Criteria-compliant Protection Profiles will be developed to foster development and evaluation of security products used to comprise ICSs. The protection profiles and developed products can be evaluated through oversight provided by NIAP.

NIAP is the US organization that operates a security product evaluation program that complies with international CCRA requirements. The CCRA provides the means for the results of security product evaluations to be recognized by all countries that participate in the CCRA. Through NIAP, a vendor may have a product evaluated in the US and have the results of that evaluation recognized in other countries. This minimizes the time, expense and resources required to demonstrate assurance in the security capabilities of a product for application in diverse operational environments. Likewise, the results of a security product evaluation performed outside the US by a country participating in the CCRA will be recognized by NIAP. Additional information on NIAP may be found at www.niap.nist.gov and additional information on the CCRA and the participating countries may be found at www.commoncriteria.org.

1.6.5. Relationship to other industry-specific initiatives and standards organizations

The various industrial control sectors and relevant standards organizations each have initiatives targeted at defining sector-specific guidance and best practices for developing and operating security programs or for implementing security technologies into their ICSs. The relationship between the sector-specific initiatives and this document is very much like that of SP99 and this document: Where sector-specific efforts have developed detailed statements of security technology capabilities, that information may either be incorporated into a refinement of this document or referenced by the refinements of this document. Where sector-specific efforts have developed security program guidance and industry practices for implementation within their industry, the information collected from those actions can be used to develop refinements of this document.

1.7. Reading this Document

Throughout the document there is explanatory discussion provided to aid the reader in understanding the material presented and in correlating the security-focused discussion into practical contexts. All such text is preceded by the header *Application Note* and is presented in an italicized font to distinguish the text from the main document text. The application notes can be broad in scope as they strive to address all stakeholder communities of interest: acquisition; vendors; integrators; operations and maintenance; test, evaluation and certification; policy and other mandate directorates, both governmental and industrial.

2. ICS System Definition and Description

This section defines the components of a control system in an abstract manner. The abstraction allows subsequent sections to discuss the security issues independent of the attributes specific to control system vendor products. This section does not address the security capabilities of systems that are external to the control system. Examples of these systems include enterprise management and office automation systems. This section does, however, address the security capabilities for the interfaces between the ICS and external systems.

The ICS is characterized by components that record information, monitor information, transmit information, receive information or determine and issue command sequences. An ICS is comprised of a collection of individual component types that are integrated together to manage an industrial production, transmission, or distribution process. These components may be categorized in terms of the fundamental function they provide within the ICS, such as a controller, sensor, transmitter or actuator. These components may also be characterized in terms of their basis of operation, which may be mechanical, pneumatic, hydraulic, electrical or electronic means. An additional categorization may be made when these fundamental functions are integrated together to provide multiple functions within a single physical housing, such as the combining of a sensor and transmitter function into a single physical unit.

The key control components of an industrial control system, including the control loop, the human machine interface (HMI), and remote diagnostics and maintenance utilities, are shown in Figure 3. A control loop consists of sensors for measurement, control hardware, process actuators, and communication of process variables. Measurement variables are transmitted to the controller from the process variable sensors. The controller interprets the signals and generates corresponding control signals that it transmits to the process actuators. This sequence of events results in new values of the process variables and the sensors transmit revised signals back to the controller. The human-machine interface allows a control engineer or operator to configure set points, control algorithms and parameters in the controller. The HMI also provides displays of process status information, historical, information, reports, and other information to operators, administrators, managers, business partners and other authorized users. A typical ICS contains some number of control loops, HMIs and diagnostics and maintenance tools integrated through an array of network protocols. Supervisory level loops and lower level loops typically operate continuously over the duration of a process. These may operate at cycle times ranging from milliseconds to minutes.

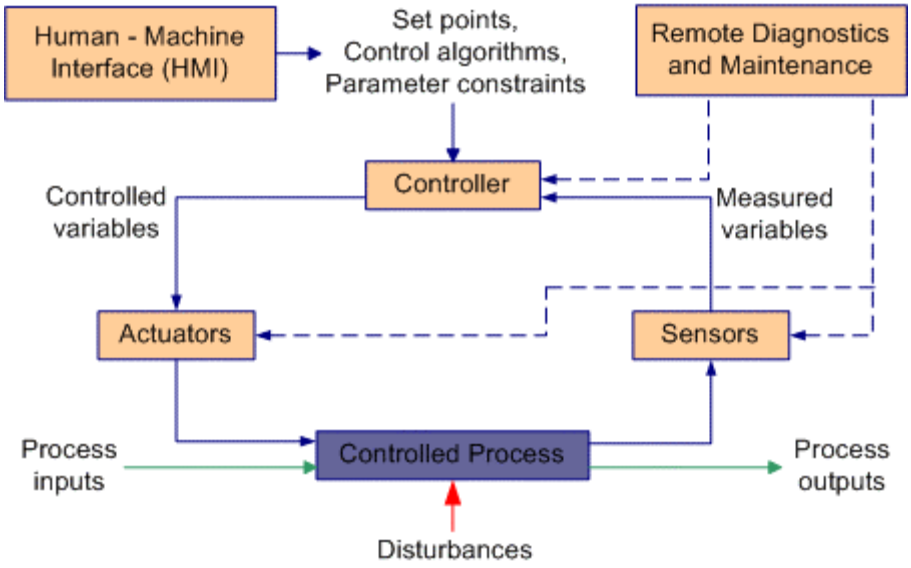


Figure 3 – Fundamental Control System Components

There are four primary commercially available industrial control system classifications:

- The programmable logic controller (PLC),
- the Distributed Control System (DCS),
- the Hybrid Control System (HCS), and
- the Supervisory Control and Data Acquisition System (SCADA).

PLCs are highly scalable modular controllers with modules available for processing, discrete I/O, and analog input and output capabilities as well as communication interfaces. DCSs, HCSs and SCADAs are more integrated systems that typically are configured to control a distributed process, where subsystems communicate over a variety of communication media (e.g. LAN, WAN, the Internet, Telephone Lines, Radio Frequency Transmissions) depending on relative proximity of the subsystems. These distributed systems typically include database historians and HMIs. DCSs and HCSs are similar, however HCSs are typically smaller systems and are tightly integrated by a single vendor and include a "built in" database, historian, HMI and programming environment. Distributed systems that control processes that are distributed over large geographical areas are typically categorized as SCADA systems. A DCS, HCS, and SCADA system can contain several PLCs.

PLC's are used to control discrete processes and are also used to control subsystems in DCS, HCS and SCADA systems. DCS and HCS are used to control large, complex processes such as power plants or refineries, typically at a single site. SCADA systems typically control less complex, but more dispersed assets where centralized data acquisition is often more important than control. Typically, distribution operations of water systems, gas pipelines, and electrical transmission lines use SCADA systems. Generic industrial control system network architectures are shown for both DCS and SCADA based control schemes in the Appendix I. A glossary of terms describing the components found in the diagrams is available in Appendix II of this document.

Despite the different nomenclature, the underlying concepts, components, and functions of PLC, DCS, HCS and SCADA systems are similar. Therefore, this document targets the ICS in an abstract sense – it might be one of the systems described above, or some combination of these or other configurations.

2.1. Operational Security Environment

The security environment establishes the context in which the ICS operates and includes a description of the organizational assets requiring protection and the definition of what those assets need to be protected from. It is described in terms of technical controls and administrative controls. The technical controls are technology-based (i.e., the computer and communications hardware, software and firmware) while administrative controls are non-technology-based (i.e., physical controls, personnel, policies and procedures). The discussion is presented primarily in terms of assumptions, potential vulnerabilities, regulatory mandates and policies as they relate to the security environment.

- Assumptions – The assumptions regarding the intended operational environment serve to bound the problem space and problem definition. They are expressed relative to the physical and computer operating environment, the technology employed in control systems and the common and unique aspects of the varying process control industries that will make use of this specification.

- Potential Vulnerabilities – The statement of potential vulnerabilities itemizes to the types of activities that the ICS should protect against. Statements of potential vulnerabilities are made within the context of the stated assumptions and regulatory mandates and policy. Vulnerabilities apply to the control system as well as to the systems to which the control system interfaces and the physical procedures that govern the use of the control system.

- Regulatory Mandates & Policy[7] – Mandates, policies or directives that govern the use and application of control systems are stated since they may require mechanisms to support the enforcement of the criteria. These may be independent of the actual environment but rather reflect requirements placed on the organization from external entities. It may be the case that these mandates or policies conflict with the assumptions, in which case it must be resolved which take precedence so that requirements may be derived.

[7] Although regulatory information may not explicitly discuss security, it may impose other constraints that have an effect on the manner in which security solutions are engineered. All information related to the control system must be reviewed such that security capabilities do not conflict with other requirements and capabilities of the system.

2.2. Secure Usage and Environment Assumptions

Assumptions are axiomatic statements about the intended usage of the ICS within the operational environment that affect the security of the ICS. These assumptions state a condition that is to exist in the environment of the implemented ICS but are not part of the ICS. These are used to mitigate the extent to which the ICS must meet all the security objectives within the operational environment. They define those measures that the ICS can expect to exist and rely upon to achieve the overall level of security sought.

2.2.1. Control_System_Physical_Access

The ICS facility will provide adequate physical access protections to prevent unauthorized physical access to the ICS components within that facility. .

Application Note: This assumption is not intended to imply that just because an individual is granted physical access to the facility they have unrestricted access to all portions of that facility. It is expected that there may be varying degrees of physical barriers to the different portions of the ICS. For instance, physical access to the HMI will be different than to a fielded device of the ICS.

Application Note: Some companies have defined a logical concept called the "Operating Area" which is defined as including any physical location from which operations tasks or commands may originate. Typically, this is synonymous with the control room, but with things such as wireless control devices and roving operators, this may not always be the case. Another example would be a remote product loading station. The logical sum of that location and the control room would constitute the "Operating Area".

2.2.2. ICS_External_Network_Connectivity

The ICS network may have connectivity with non-ICS system networks through which Internet connectivity is possible.

Application Note: The implication is that the control system may be accessed via an external electronic connection and that internal access to the control system is possible from other facility networks.

2.2.3. Remote_Access

Remote access to ICS components may be available to authorized individuals.

Application Note: Authorized individuals include product vendors, integrators, maintainers as well as personnel employed at the process control facility.

2.2.4. No_Infrastructure_Security_Services

There are no security services provided by the communications infrastructure for the ICS components.

Application Note: There are no expectations for communication mediums to be secure. There are also no expectations that any security may be derived from components that implement the communications infrastructure.

2.3. Potential Vulnerabilities

The statement of potential vulnerabilities establishes a basis for the derivation of specific security capabilities to be implemented by the ICS. Potential ICS vulnerabilities have been derived from PCSRF meetings and ICS sector-specific workshops. Each statement of vulnerability has relevance to at least one of the following contexts:

- Intended operational environment of the ICS components;
- Purpose, function and use of the ICS components;
- Technology employed in ICS components;
- Communication medium employed to provide connectivity between ICS components;
- Human agents with intent to monitor, disrupt, destroy or incapacitate ICS operation;
- Natural disaster events that can disrupt or destroy an ICS operation.

The following statements provide a characterization of the potential vulnerabilities of concern that may be exploited for the intent of disrupting or otherwise preventing an ICS from accomplishing its designed intent.

2.3.1. Unauthorized Analysis

- information stored on an ICS component may be accessed and analyzed without authorization.

- information flows between ICS components are intercepted and analyzed by unauthorized individuals.

2.3.2. Unauthorized Insertion

- information stored on an ICS component may be modified without authorization.

- information flows between ICS components are intercepted and replayed

- information flows between ICS components are intercepted, modified, and replaced back on the network.

- information flows between ICS components are inserted

- unauthorized executable code is uploaded to an ICS component.

2.3.3. Unauthorized Removal

- information stored on an ICS component may be deleted without authorization.

2.3.4. Fault-Detection

- faults that occur within the ICS are not detected and therefore cannot be acted upon.

2.3.5. Denial of service

- authentic ICS communication is prevented from reaching its destination by flooding of the communications.

- authentic ICS component actions cease to function due to flooding of the component.

2.3.6. Integrity

- an illegal command that exceeds the privileges of the entity is issued by a user or ICS component.

- an illegal command that modifies the system configuration of an ICS component to provide an existing user, new user, or system with rights that exceed the intended authorized rights is issued by a user.

2.3.7. Availability

- an ISC component may cease operation due to being damaged or taken out by a malicious attack or natural event.

- an ISC communication may cease operation due to being damaged or taken out by a malicious attack or natural event.

2.4. Regulatory Mandates & Policy

Regulatory mandates and policy statements are the basis for stating capabilities that must be implemented by the ICS. These capabilities are constraints imposed on ICS operations by governmental, industry-specific or other entities with jurisdiction over the control industry and its ICS operations.

This polices in this section should have overlap and consistency with related control system industry security initiatives that provide, establish or recommend best practices, policies and procedures for secure ICS operations (e.g., SP99).

2.4.1. Safety_Dependency

ICS security capabilities implementation shall include securing the interfaces and interconnectivity of the ICS safety systems.

2.4.2. Operational_Non_Interference

ICS security capabilities shall be implemented so as to not impede the bare minimum operational capability of the ICS and so as to not impede the safety systems that protect the ICS.

Application Note: The interpretation of the term "bare minimum" varies for different ICS sectors and varies within a single ICS implementation. Bare minimum includes, but is not limited to, real-time constraints (e.g., handling interrupts), bandwidth constraints and resource constraints (e.g., processor or memory).

2.4.3. Risk_Assessment

The ICS shall be designed, implemented, and operated to meet the risk objectives resulting from a system life-cycle risk management program. The risk management program shall establish a comprehensive and integrated set of risk management goals for issues affecting ICS operation, ICS safety and ICS security.

2.4.4. Business_Continuity

The ICS shall be operated in accordance with a business continuity policy that addresses the identification of and response to events that adversely affect the ability of the ICS to operate in fulfilling its design goals.

3. Industrial Control System Capability Objectives

This section documents the capability objectives that must be met by a compliant ICS. The capability objectives apply to both the technology-based components of the ICS and to the non-technology physical controls, personnel and procedures of the ICS. In addition, for the non-technology objectives these may be part of the operational environment in which the ICS is implemented.

3.1. ICS Non-Technical Operations Objectives

3.1.1. Business_Continuity

The ICS shall ensure continuity of operations in accordance with a business continuity policy that addresses a known set of anticipated events that might adversely affect the operational capability of the ICS.

Application Note: The business continuity policy should address a known set of anticipated events that could happen, what the implications are when an event happens, and what the recovery actions are when those events happen. The focus of a business continuity policy is likely to vary to some extent with respect to the security properties of availability, confidentiality and integrity depending on the set of events anticipated for a particular installation.

3.1.2. Regulatory_Compliance

The ICS shall be operated in compliance with relevant governing mandates.

Application Note: The issue of ensuring compliance with regulatory mandates requires identification of such mandates and the assessment of how to incorporate the appropriate language in the requirements spec to ensure that such compliance may be demonstrated.

3.1.3. Risk_Assessment

ICS risk assessments shall be conducted throughout the life-cycle of an ICS, such that:

- A documented and approved risk assessment process is conducted initially for the ICS and reviewed with each change to the manufacturing process or ICS change.
- The results of the risk assessment are relevant to and are applied throughout the control system life cycle process,
- The control system general operating environment and application of security technology is periodically updated, to ensure that changing vulnerabilities do not degrade the security of the ICS.

Application Note: Risk assessment activity must be done prior to development, updated during development as required, and then on an agreed periodic basis during operational use.

3.1.4. Security_System_Verification:

The ICS components and as an integrated system shall be capable of undergoing verification analysis and testing to ensure that the ICS:

- Meets its security design specification
- Is properly installed and integrated
- Is properly configured

3.1.5. Security Migration_Strategy

The ICS shall have a migration strategy providing the capability to govern the evolution of the control system throughout its security operational life-cycle. The migration strategy shall address at a minimum:

- Assessment of new vulnerabilities and appropriate/necessary mitigating actions to control/reduce new vulnerabilities. This may include maintenance of the current system state (components, configuration, patches, etc).
- The integration between computer implemented and personnel implemented procedures.

3.1.6. Collaborative_Working_Relationships

Policies governing the roles, responsibilities and activities authorized for individuals not employed by the control system operating organization shall be developed.

The policies shall establish methods for on-site internal, on-site remote, and off-site remote access to control system resources.

Application Note: There is need for well-defined rules governing the interaction with business partners of the ICS organization and the action taken should the rules be violated.

3.1.7. Security_Ownership

A policy for governing security shall be defined to establish the following:

- an organization-wide, security management infrastructure
- identified roles and responsibilities, together with explicit authority, to ensure security of operation within the management infrastructure

The policy shall define the offices, their interrelationships, and their responsibilities for the security of all control system and non-control system computer resources and the roles authorized to manage those resources.

Application Note: There is a need for a clear chain of authority with responsibility for the management of all ICS operations and security, and to remove the top-level distinction between control and IT systems.

3.2. ICS Technology-Based Objectives

The following ICS technology-based objectives establish the high-level statement of functional security capabilities that are to be met through combinations of hardware, software and firmware.

3.2.1. Non_Interference

The ICS security functions shall be implemented in a non-interfering manner such that behavior of the ICS functions and safety functions are able to meet their performance constraints.

3.2.2. Security_Override

The ICS shall provide the capability for the controlled bypass of security mechanisms in those instances when security policy enforcement conflicts with the continued safe and/or efficient operation of the ICS.

Application Note: This objective requires that designed over-ride mechanisms be in place to ensure that a safety-critical state is not created or an existing safety-critical state is not worsened due to security protection mechanisms.

The "controlled bypass" aspect of the objective means that the security policy includes the ability to override the security enforcement mechanism. The specific details regarding the bounds and conditions for the override capability should be stated. The event of bypassing the security mechanism shall be automatically recorded.

3.2.3. Access_Control

The ICS shall provide the capability to grant or deny access to control system resources based upon the action being performed, and the authorizations associated with authorized subjects.

Application Note: A subject is an individual or role, or a process acting on behalf of an individual or role.

- The ICS shall deny unauthorized agents access to every control system resource.

- The ICS shall require that each agent authorized to use the control system is identified and is provided with credentials to authenticate their identity.

- The ICS must be able to include knowledge of the control system state and/or the controlled process state when making an access control decision.

- The ICS shall include knowledge of time and location in the rules for making an access control decision.

3.2.4. Communications_Integrity

The ICS shall provide the capability to prevent or detect, as required, the loss of integrity of the ICS operational communications capability.

- The ICS shall provide the capability to allow information flows only between authenticated and authorized endpoints.

- The ICS shall provide the capability to protect information flows from replay, substitution or modification.

- The ICS shall provide the capability to allow the recipient of an authorized information flow to verify the correctness of the received information.

3.2.5. Control_System_Integrity

The ICS shall provide the capability to prevent or detect, as required, the loss of integrity of the ICS operational system configuration and capability.

- The ICS shall provide the capability to restrict access to the functions used to establish and maintain the secure operational configuration of the ICS.

- The ICS shall be capable of performing self-tests to verify the configuration and integrity of the security functions of the ICS.

- The ICS shall provide the capability for self-test to be executed on startup, at periodic intervals, and on demand.

- The ICS shall be capable of responding to integrity failures.

Application Note: The specific capability is left at an abstract level as the response will vary according to specific installations, i.e. it may be as simple as illuminating an indicator;

sending a message; or the response may be as complex as automatically taking corrective action to contain the failure (fail secure or reconfigure for degraded mode operation).

3.2.6. Event_Trace

The ICS shall provide the capability to record and maintain event traces that reflect the successful and unsuccessful security relevant activities involving ICS resources.

Application Note: The specific discussion focused on audit and there are some considerations that must be addressed, such as, what does audit mean in a control system context (i.e., what type of activity and what types of events are recorded) there were no unique issues brought up. This issue is closely related to the Control Systems Intrusion Detection System (CIDS) issue since the detection capability might utilize event traces as a means to detect potential policy violations.

3.2.7. Intrusion_Detection

The ICS shall be capable of detecting unauthorized activity, unusual activity and attempts to defeat the security capabilities of the ICS.

Application Note: The ICS security policies establish the basis for what is considered 1) authorized, 2) usual and 3) that result in enabling and configuring security mechanisms. Therefore, this objective is tied directly to the defined policies enforced by the ICS.

The control system shall be capable of initiating action in response to the detection of a potential violation of the ICS security policy.

Application Note: There was discussion regarding need for proactive response to an attack. Proactive response to an attack is considered as meaning automatic response to an attack, that is, without human intervention. The need for capabilities to monitor activity on the control network and to detect activity that is outside "normal parameters" requires 'normal parameters' to be defined. By defining the pattern of usage with respect to the various activities, users/subjects engage in then a "profile" of usage can be established and then will it be possible to detect potential violations of policy (i.e., an intrusion). The policy would then define the required response to each potential intrusion.

3.2.8. Operational_Configuration_Integrity

The ICS shall provide the capability to determine, maintain, and control the current configuration of an ICS component.

- The ICS shall provide the capability for a controlled update to the current configuration of an ICS component.
- The ICS shall provide the capability to restrict the use of the controlled update function

3.2.9. Availability

The ICS shall have continuity of availability of operational capability.

- The ICS shall be capable of continuing operation if a control server is unavailable for any reason.

- The ICS shall be capable of continuing operation if the primary communications channel is unavailable for any reason.

4. Control System Component Security Capability Requirements

This section documents the requirements to be met by the ICS. The requirements are grouped as they might apply to the entire ICS, to an ICS subsystem or to one or more ICS components. The scope of the requirements fall into the following categories:

- Documentation
- Configuration Management
- Access Control
- Integrity
- Functional Security Testing
- Penetration Testing, Vulnerability and Risk Assessment

The following requirements will be selected depending on the needs of a particular instantiation of an ICS. The requirements will be met in some combination by the vendor, integrator of the ICS (e.g. design documentation) and the operational facility (e.g. residual risk assessment) in which the ICS is being implemented.

4.1. Security Functional Implementation Requirements

4.1.1. ICS Security-Related Event Recording and Auditing

a. The ICS shall provide a capability to record security relevant events.

b. Each recorded event shall include the following information to support post-event analysis or reconstruction of ICS activity.
   i. Event timestamp (date and time)
   ii. Event description
   iii. Verdict depicting result of the event (e.g., success, failure)
   iv. Identity of participant(s) in the event (e.g., device, individual, role)
   v. Event-specific explanatory information

c. The ISC shall provide the capability to visually display security alarms export security alarm information in a documented format, and to notify one or more individuals of an alarm.

d. The ICS shall provide semi-automated or fully automated capabilities to review the event audit trial for identification of potential security policy violations.
   i. Selection of events to audit based upon attributes specific to the events to be recorded
   ii. Searching of events based upon attributes specific to the recorded events

Application Note: Each component shall in addition to locally recording the security event shall send the event information to a central database located on an ICS device. The

event data in this device shall be accessible through the ICS HMI for review as noted above.

e. The ICS shall provide semi-automated or fully automated capabilities to send a notification for each potential security violation as follows:
    i. For a set of security violations, the alarm shall be immediate and be available for user access in the same manner as process alarms.
    ii. For a set of security violations, the alarm shall be verified prior to the notification being made

Application Note: Semi-automated capability provides the opportunity for some prioritization in dealing with alarms, by building in operator intervention.

f. The ICS shall provide the capability to manage the behavior of the event generation and recording capabilities
    i. Startup, shutdown, backup, recovery
    ii. Selection of events to audit based upon attributes specific to the events to be recorded
    iii. Searching of events based upon attributes specific to the recorded events

g. The ability to modify the behavior of the event generation and recording capability shall be restricted to authorized individuals.

4.1.2. Communication Channels and Interconnects

a. A secure channel between communicating devices shall be established prior to any information being passed between device pairs.

b. The secure channel shall be defined as follows:
    i. Each endpoint of the communication shall authenticate the other endpoint
    ii. Information flow between the authenticated endpoints shall occur in accordance with specific rules defined for that secure channel.

c. The information flow rules shall address
    i. Data content type, form and attribute values
    ii.
    iii. Flow direction and conditions for authorized flows

d. The secure channel shall be maintained to ensure:
    i. each endpoint shall accept information received from an authenticated endpoint that is authorized to transmit the received information
    ii. each endpoint shall reject information received from
        i. a device that is not authenticated
        ii. a device that is not authorized to transmit the received information
    iii. Loss of connectivity results in attempts to reestablish the secure channel

iv. Endpoints shall detect and reject incorrectly formed and erroneous data
v. Endpoints shall detect and reject data that is inserted without authorization
vi. Endpoints shall detect and reject data that is modified (loss of integrity) without authorization
vii. Endpoints shall institute recovery action when incorrectly formed or erroneous data is received
viii. The behavior of the secure channel shall be managed by authorized individuals
ix. Each device shall authenticate the individual attempting to modify the behavior of the device prior to acting on any behavior change commanded by that individual
x. Each device shall be capable of accepting only legitimate commands and command attribute values

4.1.3. Boundary Defense Devices

a. A boundary defense device shall be capable of controlling the flow of information across its external interfaces.

b. The boundary defense device shall be capable of explicitly allowing or explicitly denying information flow based on a set of rules that address
   i. The type of information (e.g., command action, status request, configuration request)
   ii. The source identity of the information (device, individual)
   iii. The destination identity for the information (device, individual)
   iv. The protocol used
   v. The communication channel or port through which the information passes
   vi. The time and date
   vii. [other parameters]

c. The boundary device shall be capable of generating events associated with the flow of information across its interfaces
   i. Each generated event shall include the disposition of the information flow
   ii. Each generated event shall include attributes of the information flow

d. The behavior specified by the information flow rules shall be managed by authorized individuals
   i. The boundary device shall authenticate the individual attempting to modify the information flow rules prior to accepting any modifications to the rules
   ii. The boundary device shall record the actions of the authorized individual who modifies the information flow rules

iii. The boundary device shall be capable of accepting only legitimate commands and command attribute values

Application Note: A boundary defense device is a device that establishes a point of separation between two or more interconnected networks. The boundary device provides functions to monitor and control the flow of information (operational, maintenance, command) between the networks.

4.1.4. Network Addressable Field Devices

a. The network addressable field device shall be capable of identifying and authenticating itself to devices it interfaces with.
b. The network addressable field device shall be capable of responding to operational, performance and maintenance commands provided by or from an external device.
    i. The network addressable field device shall accept control system operational, performance and maintenance commands from authenticated sources
    ii. The network addressable field device shall reject control system operational, performance and maintenance commands from sources that cannot be authenticated
    iii. The network addressable field device shall be capable of qualifying each command prior to performing the commanded action
        i. A command shall be rejected if it places the device in an unsafe state
        ii. A command shall be rejected if it places the device in a non-secure state

Application Note: An unknown state may be treated as either an unsafe or non-secure state.

c. The network addressable field device shall be able to verify the integrity of its operational hardware, software and firmware base.
d. The network addressable field device shall be able to detect potential violations of the security policy that it enforces.

Application Note:
This requirement is not applied as an absolute such that every aspect of the security policy being enforced is also a candidate for determination of a potential violation.

e. The network addressable field device shall be able to determine that it has been initialized into a secure operational state prior to accepting control system operational, performance, or maintenance commands.

f. The network addressable field device shall be capable of failing into a secure state.

Application Note: The secure state may allow for continued operation albeit in a degraded or reduced capability mode. The secure state may result in cessation of all processing and communication capability, effectively resulting in a "fail-stop" halt condition.

g. The network addressable field device shall be capable of recovering from a failed secure state to an operational secure state.

Application Note: Operational secure state may be a maintenance state or a control system operational state.

h. For first time initialization, the network addressable field device shall initialize into a limited capability secure state.
    i. The network addressable field device shall require the selection and use of non-default authentication credentials;
    ii. The network addressable field device shall require explicit authorization prior to establishing communication with other devices.

Application Note: The definition of limited must be provided for each device type to which the requirement applies.

4.1.5. User Interface

a. The user interface shall be capable of authenticating individual ICS users based on each of the following or combinations of the following attributes:
    i. Unique individual identity
    ii. Role independent of individual identity
    iii. Role associated with individual identity
    iv. Location of the individual
b. The user interface shall maintain capabilities that are associated with individuals or associated with roles.
c. The user interface shall allow an individual to have authorizations for multiple roles.
d. The user interface shall provide the capability to prevent an individual from obtaining multiple roles simultaneously.
e. The user interface shall provide the capability to require an individual to explicitly request a change in role.
f. The user interface shall provide the capability for role or authorization restrictions to be overridden.
    i. The use of the override capability shall be recorded.
    ii. The override capability shall have a configurable time span after which the previously established authorizations shall be reinstated.
g. The user interface shall be capable of protecting an authorized control session from unauthorized use
    i. The user interface shall provide a configurable capability to lock the active session
        1. Mandatory session locking shall occur when the configured time of inactivity is exceeded.
        2. Operator-defined session locking shall occur by explicit operator action
    ii. The user interface shall provide the capability for re-authentication of the individual

iii. Re-authentication shall be required prior to issuing a set of commands.
iv. Re-authentication shall be required prior to accessing specific information
v. Authentication and re-authentication shall be implemented with an appropriate strength mechanism.
vi. Single factor authentication based upon a user id and password or user id and PIN shall require
    1. Minimum character length for passwords and minimum number of digits for PIN sequences
    2. The use of combinations of upper and lower case alpha characters and punctuation/special characters for passwords
vii. Two-factor authentication employing challenge-response or on-time-password hardware tokens shall have an appropriately sized pseudo-random number generator
viii. Two-factor authentication employing encryption technology shall
    1. employ encryption key lengths of sufficient length to provide the required strength for the encryption algorithm used
    2. employ certified encryption algorithms

Application Note: While the strength of a specific encryption algorithm/key length combination may be quantified, the concept of an "appropriately strong" algorithm/key length combination for a specific application context is subjective. The intent of the requirement is to ensure that thought is given to the selection of the encryption mechanism and for there to be evidence that supports that selection.

ix. Two-factor authentication employing biometric technology shall provide the capability for configuration of the false acceptance rate and false rejection rate parameters.

Application Note: An example of how these requirements might be utilized is as follows. Every time an operator invokes any action on a HMI device such as at an operator console, the device securely authenticates that the user is who he/she says they are and that this person is indeed authorized to perform that function. The authentication and authorization steps must be robust and introduce no more than an acceptable delay into the system response time. For example, both the process operator and maintenance person have a need to use the operator console to perform their work. The user interface would perform a check to establish that the person requesting an action on the console is one of these individuals. Furthermore the user interface will check that the user is authorized to perform that function. For example the operator can command the system to start making a new batch. However, the maintenance support person's request to start a batch would be ignored because this person is not authorized to do this function.

h. The user interface shall be capable of failing into a secure state.

i. The user interface shall be capable of recovering from a failed secure state to an operational secure state.

j. The user interface shall be capable of operating in a degraded mode.

Application Note: The degraded mode definition and characteristics must be defined for each instantiation. For example – assume that the user interface can no longer securely authenticate and authorize the user action. The user interface must have an override mechanism to temporarily disable these authentication and authorization steps so that the process can continue to be operated safely.

Application Note: The secure communications channel requirements identified in Section 5.12 also applies to user interface devices. A secure communications channel failure could place the user interface into a degraded mode. The user interface notifies the user and logs the security event failure (per section 5.1.1 requirements). The operator console still allows the user to view the information received over the channel, but the data is flagged by the user interface to identify the suspect security quality of the data.

k. The user interface shall provide the capability for device fail-over or device function fail-over.

4.2. Security Verification, Operation and Maintenance Assurance Requirements

4.2.1. ICS Policy Documentation

a. ICS operational policies shall be developed and maintained.

b. The ICS operational policies shall address
   i. ICS roles, responsibilities and authority regarding ICS management, operations, administration and maintenance
   ii. ICS intended usage and compliance with operations procedures
   iii. Agreements between ICS management and the management of external systems or devices to which the ICS receives or transmits information

4.2.2. Security Architecture Documentation

a. The ICS architecture shall be documented and maintained.

b. The ICS architecture documentation shall include:
   i. Physical layout of network
   ii. Definition of ICS subsystems and protection domains
   iii. Placement of ICS components in the network
   iv. Logical flows of information between ICS subsystems and components through the network
   v. Definition of interfaces and interconnects
      1) As they apply externally to ICS components
      2) As they apply externally and internally to ICS subsystems

3) As they apply externally to the ICS to enable integration with other systems or devices

4.2.3. Security Configuration Documentation

a. The operational configuration of ICS components shall be documented and maintained.

b. The ICS operational configuration documentation shall include:
   i. Component version number(s)
   ii. Unique identification of applied patches or service packs
   iii. Installation, startup, steady-state runtime, and shutdown parameters

4.2.4. Security Design Documentation

a. The design of ICS components shall be provided for use by ICS system integrators.

b. The component design documentation shall include:
   i. Definition of external interfaces
   ii. Description of behavior or functionality provided at the interface
   iii. Description of fault and error conditions
   iv. Description of secure startup and shutdown procedures
   v. Description of secure hardware, firmware or software update procedures
   vi. Description of component secure failure and secure recovery operation
   vii. Guidance governing secure installation of the component
   viii. Guidance governing secure integration of the component into the ICS
   ix. Guidance governing secure operation of the component
   x. Guidance governing secure maintenance of the component

4.2.5. System Security Testing

a. The ICS components shall be integrated and tested prior to their use to support operational control system functions.

b. An ICS test plan shall be developed and maintained.

c. The ICS test plan shall include the following:
   i. ICS integration test strategy
   ii. ICS component installation verification test procedures
   iii. ICS subsystem integration and verification test procedures
   iv. ICS system verification test procedures
   v. ICS interoperability with external devices test procedures
   vi. ICS vulnerability and penetration test philosophy, constraints and procedures

d. The test procedures shall include:

i. Testing sequence dependencies
ii. Configuration verification
iii. Expected and actual test results

4.2.6. Residual Risk Assessment

a. The ICS shall undergo periodic assessment to determine the level of residual risk.

b. The periodic assessments shall include
    i. Verification of correct configuration
    ii. Determination of new vulnerabilities
    iii. Engineering assessment and penetration testing to intentionally defeat the security countermeasures

5. Appendix I – Industrial Control Systems and Industries Overview

The following discussion attempts to provide the reader with a high level grounding on the types of process control equipment that are typically used in Industrial Control System applications. These systems are very flexible and can be applied to meet the needs of several different industry segments. The discussion is not meant to be an in-depth analysis of when to utilize the different types of process control systems.

Real-time computer control systems used in process control applications have many characteristics that are different than traditional information processing systems used in business applications. Foremost among these is design for efficiency and time-critical response. Security is historically not a strong design driver and therefore tends to be bypassed in favor of performance. Computing resources (including CPU time and memory) available to perform security functions tend to be very limited. Furthermore, the goals of safety and security sometimes conflict in the design and operation of control systems.

Digital industrial control systems are used extensively in process-based or discrete-based manufacturing industries. In general there are two main types of manufacturing processes in the process industries; continuous processes and batch processes. Some typical continuous manufacturing processes include fuel or steam flow in a power plant, petroleum in a refinery, distillation in a chemical plant. The operation runs at a steady state condition with transitions to make different grades of a product. On the other hand, batch manufacturing processes are characterized by distinct processing steps conducted on a quantity of material. There is a distinct start and end to the series of steps with possibly some brief steady state operations on a given step of the process. The discrete-based manufacturing industries typically conduct as series of steps on a single device to create the end product. Electronic parts assembly is a typical example of this type of industry. Both industry segments utilize the same types of control systems, sensors, and networks. While efforts of the PCSRF are currently geared toward control systems for the continuous processing industries, results will likely be applicable to control systems used in the discrete-based industries.

The computer control systems used in process industries, including electric utilities, petroleum (oil & gas), water, waste, chemicals, pharmaceuticals, pulp & paper, and metals & mining can be divided amongst the usage of either DCS, PLC or SCADA technology and implementation depends on the geographic distribution of the operation. Network architectures that encompass processing operations involving the transformation of raw materials into a usable product in a continuous fashion follow the DCS scenario. On the other hand, the network architectures that encompass distribution operations of the usable products, typically over large distances, follow the SCADA scenario.

The electrical power infrastructure is made up of power generation facilities as well as transmission and distribution networks (electric power grid) that create and supply electricity to end-users. Power generation facilities include fossil fuel, nuclear power and

hydroelectric systems. Fossil fuel and nuclear plants heat water in a boiler to steam. The high-pressure steam, in turn, flows into a turbine, which spins a generator to produce electricity. Hydroelectric generation facilities utilize the force of water, via a dam, flowing into a turbine, which spins a generator to produce electricity. These generation facilities use DCS and PLC technology. The electric power grid is a highly interconnected and dynamic system consisting of thousands of public and private utilities and rural cooperatives. A SCADA system manages distribution systems by collecting the electric system data from the field and issuing control commands to the field. Many substations also use PLC technology.

Natural gas, crude, refined petroleum, and petroleum-derived fuels represent Oil and Gas substances. The Oil & Gas infrastructure includes the production holding facilities, refining and processing facilities, and distribution mechanisms (including pipelines, ships, trucks, and rail systems) for such substances. Refining and processing facilities make use of DCS while holding facilities and distribution systems utilize SCADA technology.

The water supply infrastructure encompasses water sources, holding facilities, filtration, cleaning and treatment systems and distribution systems. Like electric, oil and gas, the processing operations use DCS and PLC technology while the distribution operations use SCADA technology. A wastewater treatment infrastructure is very similar to that of a water supply infrastructure. Chemical, pharmaceutical, pulp and paper, and metals and mining industries primarily fit into the category of processing facility and use DCS technology.

A comparison of these diagrams shows that at the higher level of the plant network architectures the plant operations are similar for plants containing either DCS, PLC or SCADA systems. At this level, everything resides on a local area network. These include general-purpose workstations, printers, plant database, application servers and domain controllers. Communication outside the plant is typically established via a firewall to the Internet or a wide area network (WAN). Modems are also available, usually to allow remote access to employees working from home or on the road and equipment suppliers for remote maintenance. The DCS, PLC and local SCADA components of a plant system typically reside on a peer-to-peer network.

5.1. DCS Component Characterization

A DCS is comprised of a supervisory layer of control and one to several distributed controllers contained within the same processing plant. The supervisory controller runs on the control server and communicates to its subordinates via a local network. The supervisor sends set points to and requests data from the distributed controllers. The distributed controllers control their process actuators based on requests from the supervisor and sensor feedback for process sensors. These controllers may use a local network link to communicate with actuators and sensors eliminating the need of point-to-point wiring between the controller and each device. There a several types of controllers used at the distributed control points of a DCS including machine controllers, PLCs, process controllers and single loop controllers depending on the application. Many of the

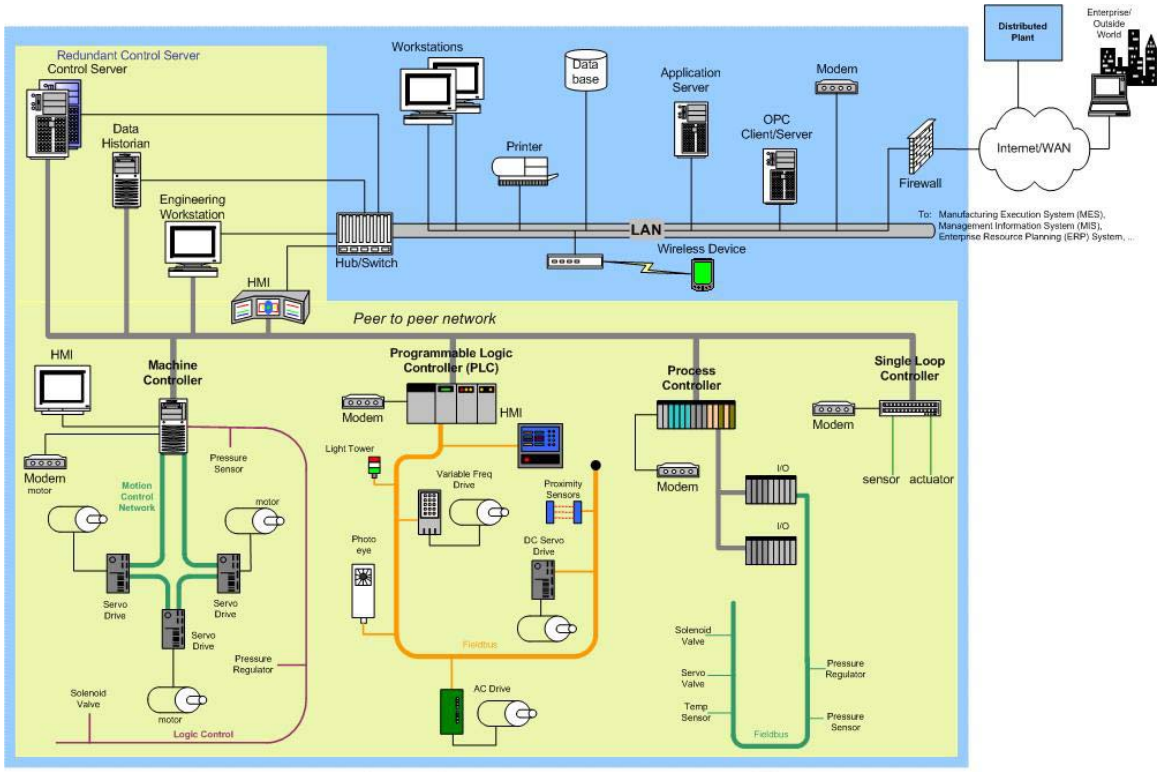
distributed controllers on a DCS have the capability to be accessed directly via a modem allowing remote diagnostics and servicing by vendors as well as plant engineers.

5.2. SCADA Component Characterization

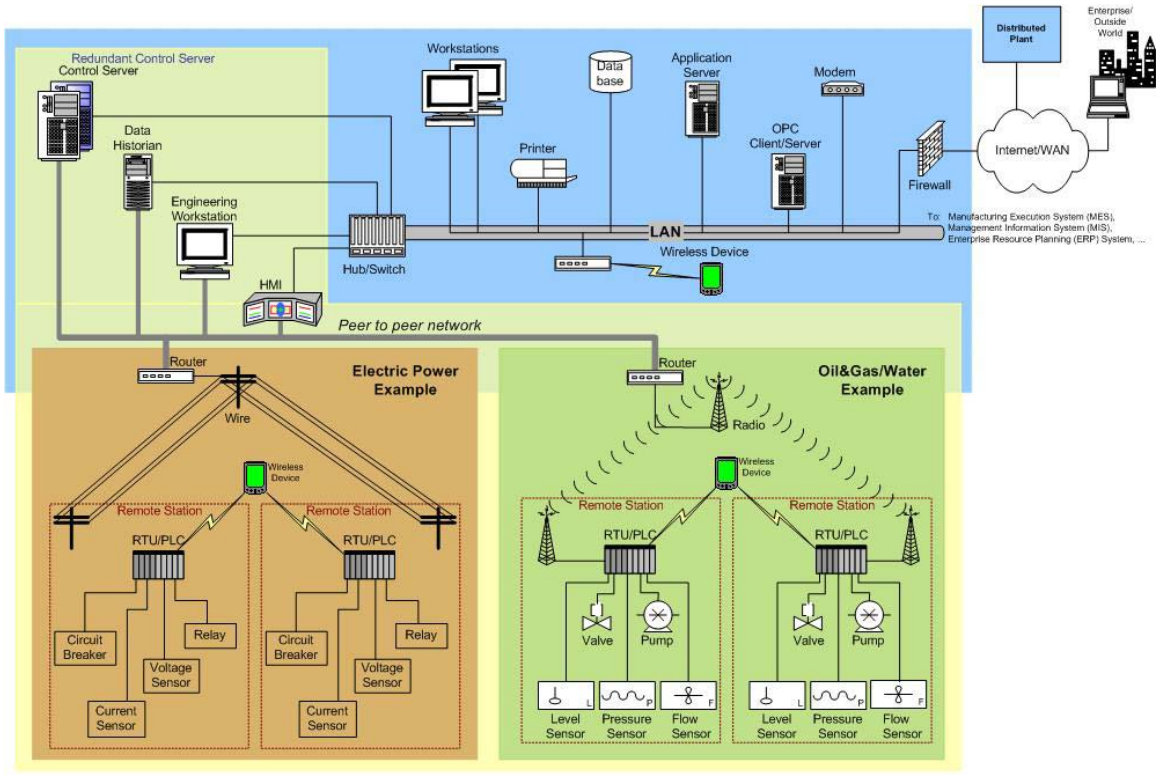
A SCADA system typically consists of a Central Monitoring System (CMS), contained within the plant and one or more Remote Stations. The CMS houses the Control Server and the communications routers via a local network. The CMS collects and logs information gathered by the remote stations and generates necessary actions for events detected. A remote station consists of either a Remote Terminal Unit (RTU) or a PLC that controls actuators and monitors sensors. Remote stations, typically, have the added capability to be interfaced by field operators via hand held devices to perform diagnostic and repair operations locally. The communications network is the medium for transporting information between remote stations and the CMS. This is performed using telephone line, microwave, cable, or radio frequency. If the remote site is too isolated to be reached directly via a direct radio signal, a radio repeater is used to link the site.

5.3. PLC Component Characterization

A PLC based system can be very similar to a DCS system in functionality. There are HMI devices, controller modules, I/O modules, and gateway devices. Typically the PLC based system is more modular in nature with the end user responsible for overall system integration. Although PLCs have analog and discrete I/O modules, the majority of applications of PLC technologies are for high speed discrete signal processing and decision-making. They can be standalone or used in conjunction with DCS or SCADA systems for specialized signal processing.



Generic Industrial Control System Network Architecture - DCS



Generic Industrial Control System Network Architecture - SCADA

1255

6. Appendix II – Glossary of Terms – Generic Composite Industrial Control System Network Architecture

AC Drive – Alternating Current Drive synonymous with Variable Frequency Drive (VFD).

Application Server – A computer responsible for hosting applications accessed and used by multiple networked user workstations.

Control Server – A server hosts the supervisory control system, typically a commercially available application for DCS or SCADA systems.

DataBase – A repository of information that usually holds plant wide information including process data, recipes, personnel data and financial data.

DC Servo Drive – A type of drive that works specifically with servo motors. Transmits commands to the motor and receives feedback from the servo motor's resolver or encoder.

Distributed Control System (DCS) – A supervisory control system typically controls and monitors set points to sub-controllers distributed geographically throughout a factory.

Distributed Plant – A geographically distributed factory that is accessible through the Internet by an enterprise.

Enterprise – A business venture or company that encompasses one or more factories.

Enterprise Resource Planning (ERP) System –A system that integrates enterprise-wide information including human resources, financials, manufacturing, and distribution as well as connect the organization to its customers and suppliers.

Fieldbus - A network that links sensors and other devices to a PC or PLC based controller and adheres to the Fieldbus standard. Use of Fieldbus technologies eliminates the need of point-to-point wiring between the controller and each device. A protocol is used to define messages over the Fieldbus network with each message identifying a particular sensor on the network.

Firewall – A devise on a communications network that can be programmed to filter information based on the protocol, source or destination.

Human Machine Interface (HMI) – The hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a color graphics display running dedicated HMI software. In this document no distinction is made between an operator console in a control room, an operator station out in the manufacturing process, a PC located in an office running the same software as is running in the control room, or a PC located off-site remotely connected to the control network running the user interface control software . All

of these scenarios are considered HMI devices providing a user with a window to the manufacturing process for viewing or control of the process.

Internet – a system of linked networks that are worldwide in scope and facilitate data communication services. The Internet is currently a communications highway for millions of users.

Input/Output (I/O) – a module relaying information sent to the processor from connected devices (input) and to the connected devices from the processor (output).

Light Tower – A device containing series of indicator lights and an embedded controller used to indicate the state of a process based on an input signal.

Local Area Network (LAN) – A network of computers that span a relatively small space. Each computer on the network is called a node, has its own hardware and runs its own programs, but can also access any other data or devices connected to the LAN. Printers, modems and other devices can also be separate nodes on a LAN.

Machine Controller – A control system/motion network that electronically synchronizes drives within a machine system instead of relying on synchronization via mechanical linkage.

Modem – A device that allows a computer to communicate through a phone line.

Management Information System (MIS) – A software system for accessing data from production resources and procedures required to collect, process, and distribute data for use in decision-making.

Manufacturing Execution System (MES) – Systems that use network computing to automate production control and process automation. By downloading "recipes" and work schedules and uploading production results, a MES bridges the gap between business and plant-floor or process-control systems.

OPC Client/Server – A mechanism for providing interoperability between disparate field devices, automation/control, and business systems.

Peer-to-Peer Network – A networking configuration where there is no server and computers connect with each other to share data. Each computer acts as both a client (information or service requestor) and a server (information or service provider).

Photo Eye – A light sensitive sensor utilizing photoelectric control that converts a light signal into an electrical signal ultimately producing a binary signal based on an interruption of a light beam.

Pressure Regulator – A device used to control the pressure of a gas or liquid.

Pressure Sensor – A sensor system that produces an electrical signal related to the pressure acting on it by its surrounding medium.

Primary Domain Controller – A Windows NT server responsible for managing domain information, such as login IDs and passwords.

Printer – A device that converts digital data to human readable text on a paper medium.

Process Controller – A proprietary, typically rack mounted, computer system that processes sensor input, executes control algorithms and computes actuator outputs.

Programmable Logic Controller (PLC) – A small industrial computer used in factories originally designed to replace relay logic of a process control system and has evolved into a controller having the functionality of a process controller.

Proximity Sensor – A non-contact sensor with the ability to detect the presence of a target, within a specified range.

Redundant Control Server – A backup to the control server that maintains the current state of the control server at all times.

Remote Terminal Unit (RTU) – A computer with radio interfacing used in remote situations where communications via wire is unavailable. Usually used to communicate with remote field equipment. PLCs with radio communication capabilities are also used in place of RTUs.

Servo Valve – An actuated valve that's position is controlled using a servo actuator.

Sensor - A device that senses or detects the value of a process variable and generates a signal related to the value. Additional transmitting hardware is required to convert the basic sensor signal to a standard transmission signal. Sensor is defined as the complete sensing and transmitting device.

Single Loop Controller – A controller that controls a very small process or a critical process.

Solenoid Valve – a valve actuated by an electric coil. A solenoid valve typically has two states: open and closed.

Supervisory Control and Data Acquisition System (SCADA) – Similar to a Distributed Control System with the exception that sub-control systems are geographically dispersed over large areas.

Temperature Sensor – A sensor system that produces an electrical signal related to its temperature and, as a consequence, senses the temperature of its surrounding medium.

Variable Frequency Drive (VFD) – A type of drive that controls the speed, but not the precise position, of a non servo, AC motor by varying the frequency of the electricity going to that motor. VFDs are typically used for applications where speed and power are important, but precise positioning is not.

Workstation – A computer used for tasks such as programming, engineering, and design.

Wide Area Network – A network that spans a larger area than a LAN. A WAN typically provides communications between LANs and may connect to on or more other WANS.

Wireless Device – A device that can connect to a manufacturing system via radio or infrared waves to typically collect/monitor data, but also in cases to modify control set points.